PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-069595**
(43)Date of publication of application : **07.03.2003**

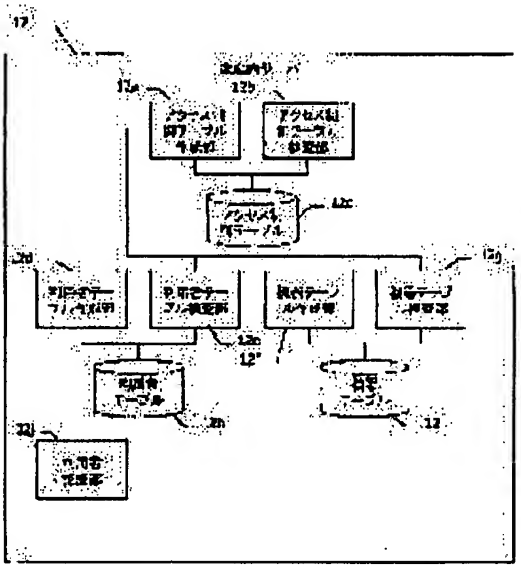
(51)Int.Cl. **H04L 12/46**
G06F 12/14
G06F 15/00
H04L 12/66
H04Q 9/00

(21)Application number : **2001-255251**
(22)Date of filing : **24.08.2001**

(71)Applicant : **SANYO ELECTRIC CO LTD**
(72)Inventor : **OKAMOTO MITSUNAGA**
INOUE YASUAKI

(54) ACCESS CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To perform a fine access control.
SOLUTION: A home server 12 having an access control table 12c, a user table 12h, and a device table 12i makes a decision whether or not to permit an access request after referring to contents of these tables when the access request about a customer premises equipment is received from external equipment. Especially, the approval or disapproval of the access request is predefined in detail about contents of functions of the external equipment, etc., thereby the fine access control can be done.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2003－69595
(P2003－69595A)
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	12/46		H04L	12/46	M　5B017
G06F	12/14	310	G06F	12/14	310K　5B085
	15/00	330		15/00	330D　5K030
H04L	12/66		H04L	12/66	B　5K033
H04Q	9/00	301	H04Q	9/00	301D　5K048

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願2001－255251(P2001－255251)

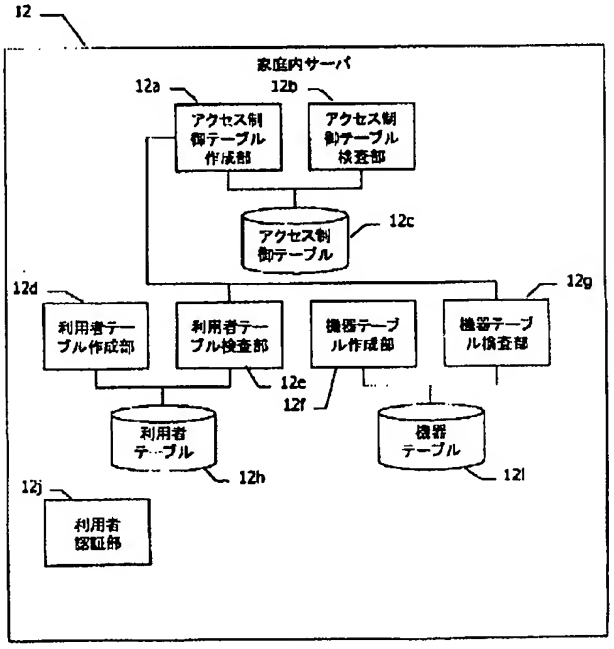
(22)出願日　平成13年８月24日(2001.8.24)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　岡本　充永
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　井上　泰彰
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

最終頁に続く

(54)【発明の名称】　アクセス制御システム

(57)【要約】
【課題】　きめ細かなアクセス管理を行う。
【解決手段】　家庭内サーバ１２は、内部にアクセス制御テーブル１２ｃ、利用者テーブル１２ｈ、機器テーブル１２ｉを有し、外部から宅内機器についてのアクセス要求がきたときに、これらテーブルの内容を参照してアクセス可否を判定する。特に、このアクセス可否は、機器の機能などの内容についても細かく設定されており、きめ細かい制御が行える。



1

【特許請求の範囲】

【請求項１】　内部ネットワークを介し接続された複数の機器と、

前記複数の機器のそれぞれについて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、

を含み、

前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御するアクセス制御システム。

【請求項２】　内部ネットワークを介し接続された複数の機器と、

前記複数の機器についてのアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、

を含み、

前記管理サーバは、外部通信ネットワークを介し接続された機器の内の１つの機器による、あるいは、前記複数の機器の内の１つの機器による、他の機器が有するオブジェクトの使用を制御するアクセス制御システム。

【請求項３】　内部ネットワークを介し接続された複数の機器と、

前記複数の機器のそれぞれについて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、

を含み、

前記管理サーバは、

外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御すると共に、外部通信ネットワークを介し接続された機器の内の１つの機器による、あるいは、前記複数の機器の内の１つの機器による、他の機器が有するオブジェクトの使用を制御するアクセス制御システム。

【請求項４】　請求項１～３に記載のシステムにおいて、

前記管理サーバは、利用者毎、または利用者のレベル毎にアクセスの可否またはオブジェクト使用の可否についてのデータを記憶しているアクセス制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続されている各種機器についてのアクセス制御に関する。

【０００２】

【従来の技術】従来より、パソコンやネットワークサーバなどにおいては、ファイルやディレクトリに対するアクセス制御が行われている。すなわち、ファイルやディ

2

アクセスを許可したり、限定されたユーザについてのみアクセスを許可するというアクセス権を設定することができる。例えば、特開２００１－６０９７２号公報では、機器の機能とユーザのレベルを組み合わせたアクセス制御方式を提案している。

【０００３】また、特開２００１－６０９７２においては、外部通信回線を介する外部端末からの内部機器へのアクセスをアクセス制御サーバが管理し、利用者に応じてアクセスできる内部機器を制限することが示されている。

【０００４】

【発明が解決しようとする課題】一方、家庭内の各種機器をホームネットワークで接続し、コントロールするシステムが提案されており、これらについても適切なアクセス制御が必要であると考えられる。特に、家庭内の機器についてもインターネットを介する外部からのアクセスが可能となっており、これに対するアクセス制御も重要である。

【０００５】ここで、家庭内の機器は、機器毎にその機能などが大きく異なっており、利用者毎にきめ細かなアクセス制御が重要と考えられる。

【０００６】本発明は、上記課題に鑑みなされたものであり、きめこまかなアクセス制御を効果的に行えるアクセス制御システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明は、内部ネットワークを介し接続された複数の機器と、前記複数の機器のそれぞれについて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、を含み、前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御することを特徴とする。

【０００８】このように、制御内容のレベル応じたアクセスを管理する管理サーバを設けることにより、きめこまかなアクセス管理を行うことができる。

【０００９】また、本発明は、内部ネットワークを介し接続された複数の機器と、前記複数の機器についてのアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、を含み、前記管理サーバは、外部通信ネットワークを介し接続された機器の内の１つの機器による、あるいは、前記複数の機器の内の１つの機器による、他の機器が有するオブジェクトの使用を制御することを特徴とする。

【００１０】このように、管理サーバが内部ネットワーク内の機器のオブジェクトの使用について管理することで、各機器のオブジェクトの適切な利用を図ることができる。

【００１１】また、本発明は、内部ネットワークを介し

ついて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、を含み、前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御すると共に、外部通信ネットワークを介し接続された機器の内の１つの機器による、あるいは、前記複数の機器の内の１つの機器による、他の機器が有するオブジェクトの使用を制御することを特徴とする。

【００１２】また、前記管理サーバは、利用者毎、または利用者のレベル毎にアクセスの可否またはオブジェクト使用の可否についてのデータを記憶していることが好適である。

【００１３】

【発明の実施の形態】以下、本発明の実施形態について、図面に基づいて説明する。

【００１４】図１は、システムの全体構成を示す図である。自宅１０には、例えば通信機能を有するコンピュータで構成される家庭内サーバ１２が設置されている。また、この家庭内サーバ１２には、ホームネットワーク１４を介し、宅内機器１６が接続されている。この宅内機器１６は、エアコン、テレビ、ビデオ、オーディオ機器、パソコン、デジタルカメラなどの電子的制御可能の機器であり、複数接続することも可能である。家庭内サーバ１２が、これらの宅内機器１６へのアクセス権を制御する。なお、各宅内機器１６は、基本的にそれぞれ個別にマニュアル操作が可能である。

【００１５】自宅１０の家庭内サーバ１２には、外部ネットワーク３０を介し、宅外機器２０が接続されている。外部ネットワークは、例えばインターネットのような公衆回線を利用したネットワークである。また、宅外機器２０は、ユーザが携帯する端末装置であり、携帯電話機や、ＰＤＡ（パーソナル・デジタル・アシスタント）などが好適である。

【００１６】このような構成により、ユーザが宅外機器２０を携帯して、外出した場合、外出先から外部ネットワーク３０を介し、自宅１０の家庭内サーバ１２に接続し、宅内機器の各種動作を制御することができる。

【００１７】図２には、家庭内サーバ１２の機能ブロックが示されている。アクセス制御テーブル作成部１２ａは、宅内機器１６についてのアクセス権を管理するテーブルを生成する。作成されたテーブルは、アクセス制御テーブル１２ｃとして記憶される。アクセス制御テーブル検査部１２ｂは、必要に応じてアクセス制御テーブル１２ｃの内容を検査する。

【００１８】利用者テーブル作成部１２ｄは、利用者毎のセキュリティーのレベルを規定するテーブルを生成する。作成されたテーブルは、利用者テーブル１２ｈとして記憶される。利用者テーブル検査部１２ｅは、必要に

【００１９】機器テーブル作成部１２ｆは、宅内機器１６毎のセキュリティーのレベルを規定するテーブルを生成する。作成されたテーブルは、機器テーブル１２ｉとして記憶される。機器テーブル検査部１２ｇは、必要に応じて機器テーブル１２ｉの内容を検査する。

【００２０】また、利用者認証部１２ｊは、外部ネットワーク３０を介し、アクセスしてくる利用者について、登録された利用者かどうかを認証する。例えば、宅外機器２０は、電子証明書を家庭内サーバ１２に送付し、家庭内サーバ１２はこの電子証明書により利用者を認証する。

【００２１】図３には、宅外機器２０の機能ブロックが示されている。利用者認証部２０ａは、宅外機器２０を操作する利用者についての電子証明書を取得するとともに、これを家庭内サーバ１２に供給する。アクセス可能オブジェクト選択部２０ｂは、家庭内サーバ１２から供給されるアクセス可能オブジェクトに応じ、利用者によって選択されたオブジェクトの情報を家庭内サーバ１２に供給する。

【００２２】図４には、宅内機器１６の機能ブロックが示されている。機器テーブル登録データ転送部１６ａは、機器テーブル作成部１２ｆに登録するためのデータを供給する。

【００２３】図５には、機器テーブル１２ｉの一例が示されている。この例では、宅内機器１６として、デジタルカメラ（デジカメ）、ビデオレコーダ（ビデオ）、テレビ、サーバ（家庭内サーバ１２）が挙げられている。家庭内サーバ１２も、そのアクセス制御以外の機能は、宅内機器１６としてのパソコンであり、機器テーブル１２ｉに挙げられている。

【００２４】そして、各宅内機器１６について、セキュリティーレベルが設定されるが、１つの機器について１つのセキュリティーレベルではなく、その内容に応じて異なるセキュリティーレベルが設定できるようになっている。すなわち、デジカメであれば、撮影、転送、コンテンツ１～３の５種類のオブジェクト別にセキュリティーレベルが設定されている。ここで、撮影はデジカメのシャッタ制御、転送はデジカメからの撮影データの転送、コンテンツ１～３は撮影コンテンツの閲覧を意味している。さらに、ビデオについては、再生、録画、テレビについては表示、サーバについては、保存、参照、コンテンツ４、５、６がオブジェクトとして挙げられている。このような各種のオブジェクトについて、個別にセキュリティーレベルが設定される。ここで、オブジェクトセキュリティーは、大中小の３段階となっている。

【００２５】なお、ＡＰＩ（アプリケーション・プログラム・インタフェース）は、各種動作を行うプログラムで、外部からの指令でＡＰＩの関数を呼び出して所定の処理を実行させる。すなわち、外部からの指令でＡＰＩ

5

【００２６】図６には、利用者テーブル１２ｈの一例が示されている。このように、各利用者Ａ，Ｂ，Ｃ，Ｄに対し、セキュリティーの大中小が割り当てられている。

【００２７】図７には、アクセス制御テーブル１２ｃの一例が示されている。このアクセス制御テーブル１２ｃでは、オブジェクトセキュリティーの大中小と利用者セキュリティーの大中小によって、アクセスを許可するか否かを示している。図中○が許可、×が不許可である。この例ではオブジェクトセキュリティーが利用者セキュリティー以下の場合にアクセスを許可するようになっている。

【００２８】図８は、宅外機器２０の認証のフローチャートを示しており、宅外機器２０からのアクセスがあった場合には、まず宅外機器からの利用者を認証する（Ｓ１０１）。次に、利用者テーブル１２ｈを検索し、認証された利用者のセキュリティーを決定する（Ｓ１０２）。

【００２９】図９には、宅外機器からのアクセスの時のフローチャートを示しており、まず宅外機器２０から宅内機器１６へのアクセス要求を受け付ける（Ｓ２０１）。次に、アクセス制御テーブル１２ｃを検索し、利用者が利用可能なオブジェクトセキュリティーを取得する（Ｓ２０２）。取得したオブジェクトセキュリティーを持ち、かつ要求された機器のオブジェクトを取得する（Ｓ２０３）。取得した複数のオブジェクトを宅外機器２０に提示する（Ｓ２０４）。そして、宅外機器２０が、提示されたオブジェクトの中から希望のものを選択して実行する（Ｓ２０５）。すなわち、機器テーブル１２ｉの中で宅外機器２０で選択されたものが実行される。なお、選択されたものが処理動作の場合、ＡＰＩが指定され、その動作が宅内機器１６において実行される。

【００３０】図１０には、予め利用者の利用できるオブジェクトについての情報を提示する場合のフローチャートを示す。このフローチャートによれば、まず宅外機器からの利用者を認証する（Ｓ３０１）。次に、利用者テーブル１２ｈを検索し、利用者セキュリティーを決定する（Ｓ３０２）。そして、利用者セキュリティーを満足するオブジェクトを利用者へ返送する（Ｓ３０３）。このようにして、宅外機器２０において、利用者認証終了後に、その利用者について利用可能なオブジェクトの情報が得られる。従って、利用者は提供された情報から、どの処理を行うかを決定することができる。

【００３１】このように、本実施形態によれば、（ｉ）宅外機器からＡＰＩを指定することで、宅内機器を直接制御することができるため、特別の内部機器操作手段を持つ必要がない、（ｉｉ）操作のみでなくコンテンツについてもそのアクセス権を管理することができる、（ｉｉｉ）アクセス権そのものにレベルを持たせているた

6

【００３２】次に、他の実施形態について説明する。図１１には、システムの全体構成を示してある。自宅１１０、ホームネットワーク１１４、宅外機器１２０、外部ネットワーク１３０は、基本的に上述の実施形態と同一である。そして、自宅１１０内の外部ネットワーク１３０とホームネットワーク１１４の間には、アクセス管理サーバ１１２が配置されている。また、宅内機器として、オブジェクトクライアントとして機能する宅内機器１１６と、オブジェクトサーバとして機能する宅内機器１１８が設けられている。なお、すべての宅内機器は、宅内機器１１６または宅内機器１１８のいずれになることもできる。

【００３３】図１２には、アクセス管理サーバ１１２の機能が示されている。アクセス管理テーブル作成部１１２ａは、宅内機器１１６についてのアクセス権を管理するテーブルを生成する。作成されたテーブルは、アクセス管理テーブル１１２ｄとして記憶される。アクセス管理テーブル検査部１１２ｂは、必要に応じてアクセス管理テーブル１２ｃの内容を検査する。また、利用者認証部１１２ｃは、宅内機器１１６、１１８をアクセスする利用者について、認証する。

【００３４】図１３には、宅内機器１１８の機能ブロックが示されており、利用者認証部１１８ａは、その宅内機器１１８の利用者を認証する。また、オブジェクトクライアント１８ｂは、利用者の指示に基づいて、宅内機器１１６のオブジェクトに対しオブジェクトのメソッドを呼び出す。

【００３５】図１４には、宅内機器１１６の機能ブロックが示されており、メソッド情報転送部１１６ａはアクセス管理テーブル１１２ｄに必要な情報をアクセス管理サーバ１１２に転送する。オブジェクトサーバ１１６ｂは、メソッド要求を受けたらアクセス管理サーバへ利用者のアクセス権があるかを問い合わせ、問い合わせ結果において、権利がある場合に要求に応え、要求されたオブジェクトについてアクセスを許可する。

【００３６】図１５には、オブジェクトアクセス管理テーブル１１２ｄの構成が示されている。このように、オブジェクトの種類（ａ，ｂ，ｃ）毎に、利用者別にアクセスを許可するか否かのデータが記憶されている。

【００３７】次に、このようなシステムの動作について、説明する。図１６に示すように、宅内機器１１６のオブジェクトサーバ１１６ｂは、提供可能なメソッドをアクセス管理サーバ１１２に登録する（Ｓ４０１）。これによって、図１５に示すような管理テーブル１１２ｄが作成される。

【００３８】次に、図１７にオブジェクトの利用の動作について示す。まず、宅内機器１１８のオブジェクトクライアント１１８ｂが宅内機器１１６のオブジェクトサーバ１１６ｂへメソッドの要求メッセージを送付する

管理サーバ１１２へメソッド要求利用者のアクセス権を問い合わせる（Ｓ５０２）。次に、アクセス管理サーバ１１２がアクセス権を検査してアクセスの可否を応答する（Ｓ５０３）。そして、オブジェクトサーバ１１６ｂがアクセスの可否を受け取り、メソッド要求を認めるか否かを決定する（Ｓ５０４）。

【００３９】このようにして、オブジェクトクライアント１１８ｂの要求に応じて、オブジェクトサーバ１１６ｂがアクセス管理サーバ１１２に、その可否を問い合わせ決定する。

【００４０】この例では、宅内機器１１８にオブジェクトクライアント１１８ｂがあり、ホームネットワーク１１４に接続されている場合を説明したが、これを外部ネットワーク１３０を介して接続してもよい。

【００４１】従って、オブジェクト毎にアクセス制御が可能になる。つまり、ビデオの再生や録画などの機器操作毎にセキュリティーを設定することができる。さらに、それらの操作の組合せに対してセキュリティーを設定することが可能になる。

【００４２】

【発明の効果】以上説明したように、制御内容のレベル応じたアクセスを管理する管理サーバを設けたことにより、きめこまかなアクセス管理を行うことができる。

【００４３】また、管理サーバが１つの機器による内部ネット内の他の機器のオブジェクトの使用について管理することで、各機器のオブジェクトの適切な利用を図ることができる。

【図面の簡単な説明】

【図１】　実施形態の全体構成を示すブロック図である。

【図２】　家庭内サーバの機能を示す図である。

【図３】　宅外機器の機能を示す図である。

【図４】　宅内機器の機能を示す図である。

【図５】　機器テーブルの構成を示す図である。

【図６】　利用者テーブルの構成を示す図である。

【図７】　アクセス制御テーブルの構成を示す図である。

【図８】　利用者認証の処理を説明するフローチャートである。

【図９】　オブジェクト利用可否を決定する処理を説明するフローチャートである。

【図１０】　セキュリティーレベルを提示する処理を説明するフローチャートである。

【図１１】　他の実施形態の構成を示すブロック図である。

【図１２】　アクセス管理サーバの構成を示す図である。

【図１３】　宅内機器１１８の構成を示す図である。

【図１４】　宅内機器１１６の構成を示す図である。

【図１５】　オブジェクトについてのアクセス管理テーブルを示す図である。

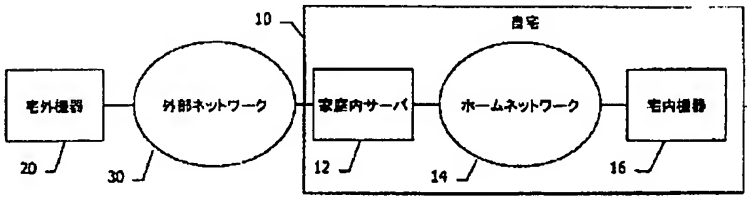
【図１６】　オブジェクトのメソッド登録に関するフローチャートである。

【図１７】　アクセル可否についてのフローチャートである。

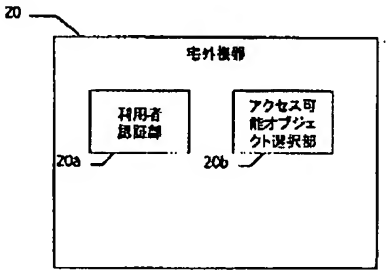
【符号の説明】

１０，１１０　自宅、１２　家庭内サーバ、１４，１１４　ホームネットワーク、１６，１１６，１１８　宅内機器、２０，１２０　宅外機器、３０，１３０外部ネットワーク、１１２　アクセス管理サーバ。

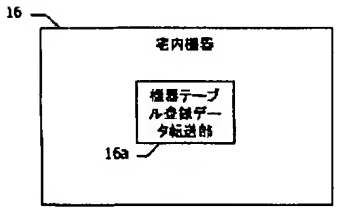
【図１】



【図３】



【図４】



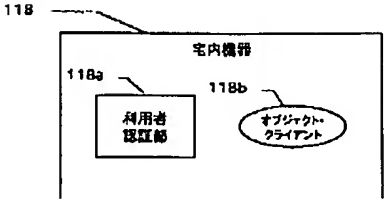
【図６】

利用者テーブル	
利用者	セキュリティ
A	大
B	中
C	小
D	小

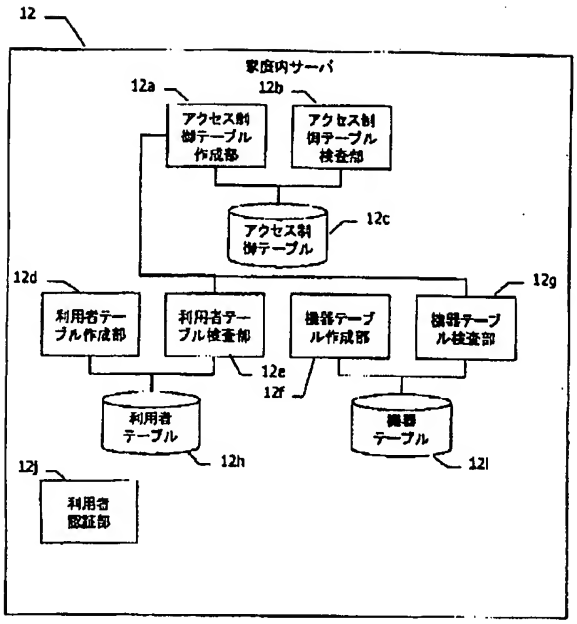
【図７】

アクセス制御テーブル		利用者セキュリティ		
		大	中	小
オブジェクトセキュリティ	大	○	×	×
	中	○	○	×
	小	○	○	○

【図１３】



【図２】

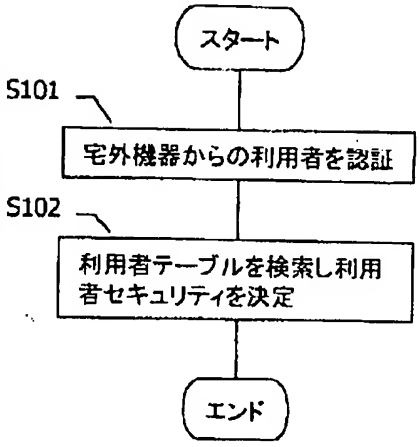


【図５】

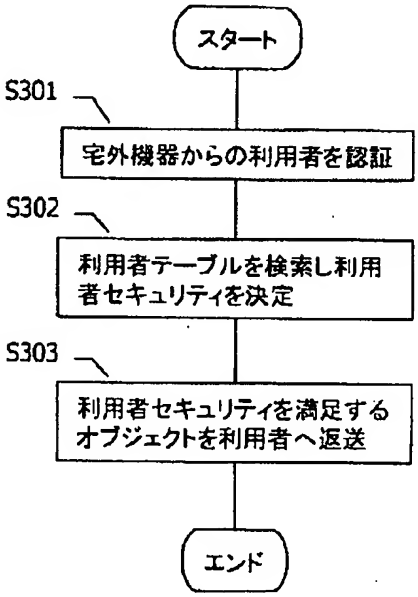
機器テーブル

機器	機能/コンテンツ	オブジェクトセキュリ	API
デジカメ	撮影	大	API1
	転送	大	API2
	コンテンツ1	小	－
	コンテンツ2	中	－
	コンテンツ3	中	－
ビデオ	再生	中	API3
	録画	中	API4
テレビ	表示	小	API5
サーバ	保存	大	API6
	参照	小	API7
	コンテンツ4	小	－
	コンテンツ5	中	－
	コンテンツ6	大	－

【図８】



【図１０】

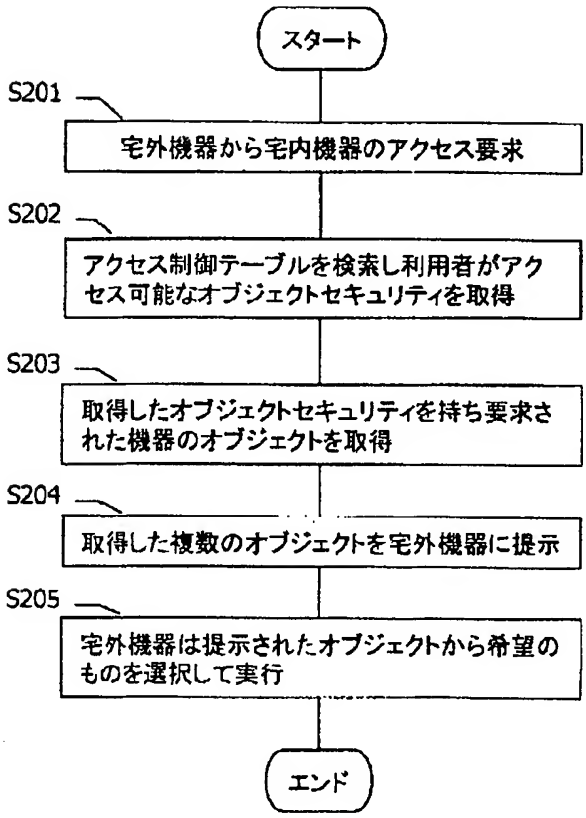


【図１５】

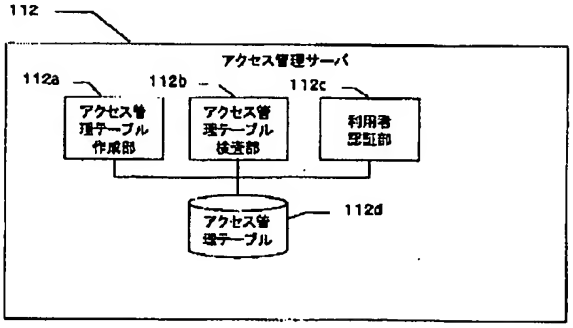
オブジェクトアクセス管理テーブル

オブジェクト		a	b	c
利用者	A	○	×	○
	B	○	○	○
	C	×	○	×

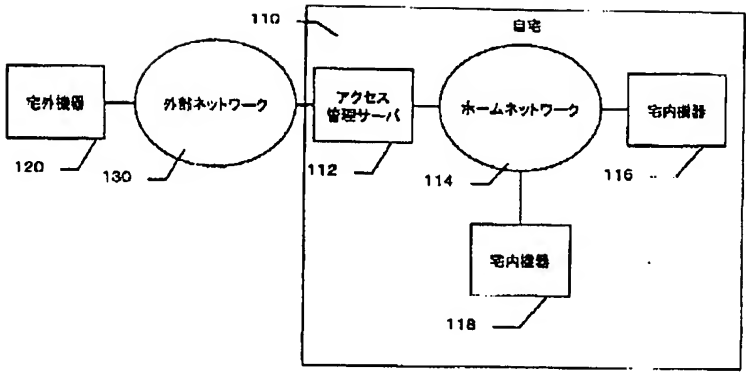
【図９】



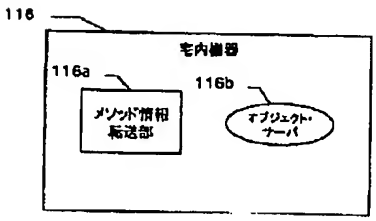
【図１２】



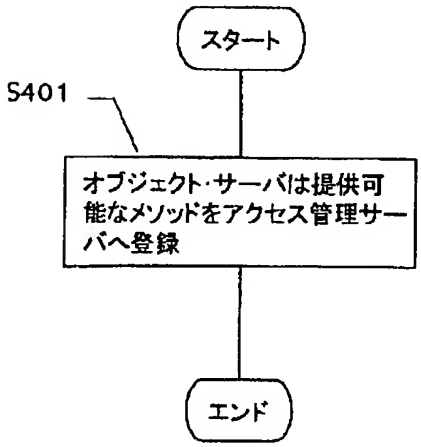
【図１１】



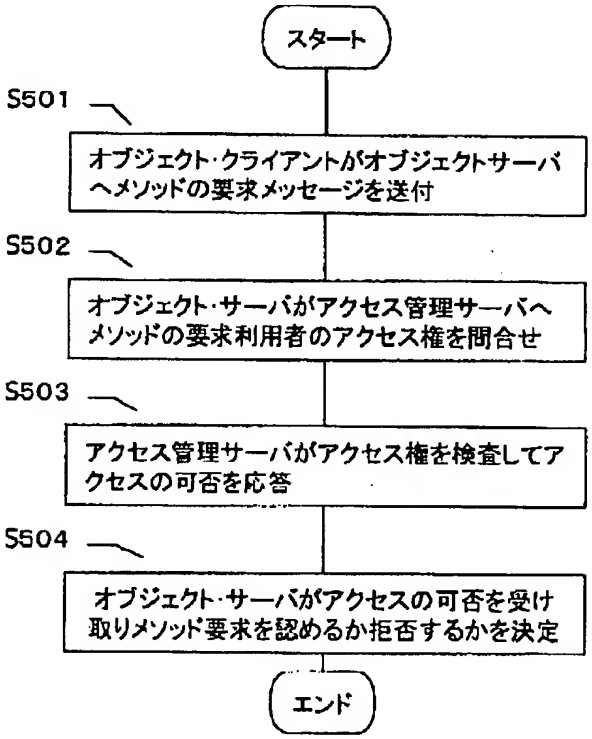
【図１４】



【図１６】



【図１７】



フロントページの続き

Ｆターム(参考)　5B017 AA07 BA06 CA16
5B085 AE06 BG07
5K030 GA15 HA08 HD03 HD06 KA01
LD20
5K033 AA08 BA01 CB08 DA06 DB12
DB14 DB16 DB18
5K048 AA15 BA01 BA13 DA05